

Art Unit: 2132

CLMPTO

11/08/04

Claims 1-3 are cancelled.

Add new claims 5-20.

4. An electronic method for delegated use of an electronic key comprising steps of:
- storing said key in a first electronic device;
  - communicating an electronic delegation certificate to a delegate;
  - sending a request and the delegation certificate from the delegate to the first electronic device; and
  - using said first electronic device to use the electronic key in response to the request and the delegation certificate.

5. A method for remotely invoking the use of a secret cryptographic key share in a process to generate a digital signature where authority to use the secret cryptographic key share lies with an authorizing entity located remotely from the cryptographic key share, the method comprising:

(a) storing the secret cryptographic key share securely in a first computational device at a first location;

(b) communicating, over a communication channel from the authorizing entity at a second location to the computational device at the first location, information that (i) identifies a document to be signed, (ii) identifies the secret cryptographic key share, and (iii) establishes authorization to use the secret cryptographic key share;

(c) at the first location, generating at least a partial result in a cryptographic process to generate the digital signature; and

(d) communicating, from the first location to a location other than the first location, the at least partial result in the process to generate the digital signature.

6. The method of claim 5 where the step of communicating an authorization to use the secret cryptographic key share includes communicating a hash of the document to be signed to the first location.

7. The method of claim 5 where the step of communicating an authorization to use the secret cryptographic key share includes a step of authenticating the authorizing entity to the first computational device.

8. The method of claim 7 where the step of authenticating the authorizing entity includes a step of signing a communication from the authorizing entity with a signature key associated with the authorizing entity.

9. The method of claim 7 where the step of communicating an authorization to use the secret cryptographic key share includes communicating a certificate identifying the authorizing entity.

10. The method of claim 5 where use of the secret cryptographic key share requires authorization from a plurality of authorizing entities, at least one of which is located remotely from the cryptographic key share.

11. The method of claim 5 where communicating from the authorizing entity at a second location to the computational device at the first location include a step of communicating information in encrypted form.

12. A method for remotely invoking the use of a secret value in a process of providing an electronic service where authority to use the secret value lies with an authorizing entity located remotely from the secret value, the method comprising:

- (a) storing the secret value in a first electronic device at a first location;
- (b) communicating, over a communication channel from the authorizing entity at a second location to the electronic device at the first location, information identifying (i) the electronic service, (ii) the secret value, and (iii) an authorization to use the secret value;
- (c) at the first location, generating an electronic result using the secret value; and
- (d) communicating the electronic result from the first location to a location other than the first location.

13. The method of claim 12 where the electronic service is the generation of an electronic signature.

14. The method of claim 13 where communicating an authorization to use the secret value includes communicating, to the first location, a hash of a document to be signed.

15. The method of claim 12 where communicating an authorization to use the secret value includes authenticating the authorizing entity to the first electronic device.

16. The method of claim 15 where authenticating the authorizing entity includes signing a communication from the authorizing entity with a signature key associated with the authorizing entity.

17. The method of claim 15 where communicating an authorization to use the secret value includes communicating a certificate identifying the authorizing entity.

18. The method of claim 1 where use of the secret value requires authorization from a plurality of authorizing entities, at least one of which is located remotely from the secret value.

19. The method of claim 12 where the secret value is a share of a secret key of an asymmetric key pair.

20. The method of claim 12 where communicating from the authorizing entity at a second location to the computational device at the first location include a step of communicating information in encrypted form.